

Richard A. Jacobsen (RJ5136)  
ORRICK, HERRINGTON & SUTCLIFFE LLP  
51 West 52nd Street  
New York, New York 10019  
Telephone: (212) 506-5000  
Facsimile: (212) 506-5151

Gabriel M. Ramsey  
(admitted *pro hac vice*)  
ORRICK, HERRINGTON & SUTCLIFFE LLP  
1000 Marsh Road  
Menlo Park, California 94025  
Telephone: (650) 614-7400  
Facsimile: (650) 614-7401

Attorneys for Plaintiffs  
MICROSOFT CORPORATION,  
FS-ISAC, INC. and NATIONAL AUTOMATED  
CLEARING HOUSE ASSOCIATION

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK**

MICROSOFT CORP., FS-ISAC, INC., and  
NATIONAL AUTOMATED CLEARING HOUSE  
ASSOCIATION,

Plaintiffs

v.

JOHN DOES 1-39 D/B/A Slavik, Monstr, IOO,  
Null, nvidiag, zebra7753, lexa\_Mef, gss, iceIX,  
Harderman, Gribodemon, Aqua, aquaSecond, it,  
percent, cp01, hct, xman, Pepsi, miami, miamibe,  
petr0vich, Mr. ICQ, Tank, tankist, Kusunagi,  
Noname, Lucky, Bashorg, Indep, Mask, Enx,  
Benny, Bentley, Denis Lubimov, MaDaGaSka,  
Vkontake, rfcid, parik, reronic, Daniel, bx1, Daniel  
Hamza, Danielbx1, jah, Jonni, jtk, Veggi Roma, D  
frank, duo, Admin2010, h4x0rdz, Donsft,  
mary.J555, susanneon, kaine habe, virus\_e\_2003,  
spaishp, sere.bro, muddem, mechan1zm,  
vlad.dimitrov, jheto2002, sector.exploits AND  
JabberZeus Crew CONTROLLING COMPUTER  
BOTNETS THEREBY INJURING PLAINTIFFS,  
AND THEIR CUSTOMERS AND MEMBERS,

Defendants.

**FILED**  
IN CLERK'S OFFICE  
U.S. DISTRICT COURT E.D.N.Y.

★ MAR 29 2012 ★

BROOKLYN OFFICE

Hon. Sterling Johnson, Jr.

Case No. 12-cv-01335 (SJ/RLM)

Courtesy Copy -

Filed by ECF

**[PROPOSED] ORDER FOR PRELIMINARY INJUNCTION**

Plaintiffs Microsoft Corp. ("Microsoft"), the FS-ISAC, Inc. (Financial Services-Information Sharing and Analysis Center) ("FS-ISAC"), and the National Automated Clearing House Association ("NACHA") (collectively, the "Plaintiffs") filed a Complaint for injunctive and other relief pursuant to, the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); violations of the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment. On March 19, 2012, the Court granted Plaintiffs' Application for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause Re Preliminary Injunction. The Plaintiffs have executed that order. Plaintiff now moves for an Order for Preliminary Injunction seeking to keep in place the relief granted by the March 19th Order, with respect to the domains, IP addresses and file paths attached hereto.

#### **FINDINGS OF FACT AND CONCLUSIONS OF LAW**

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Plaintiffs' Application for an Emergency Temporary Restraining Order, Seizure Order, and Order to Show Cause for Preliminary Injunction ("TRO Application"), the Court hereby makes the following findings of fact and conclusion of law:

1. This Court has jurisdiction over the subject matter of this case and there is good cause to believe that it will have jurisdiction over all parties hereto; the Complaint states a claim upon which relief may be granted against Defendants under the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment.

2. Microsoft owns the registered trademarks "Microsoft," "Windows," and

"Outlook" used in connection with its services, software, and products. FS-ISAC's members have invested in developing their brands, trademarks and trade names in association with the financial services they offer. NACHA owns the registered trademark "NACHA" and the NACHA logo used in conjunction with its services.

3. There is good cause to believe that Defendants have engaged in and are likely to engage in acts or practices that violate the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment

4. There is good cause to believe that, unless Defendants are restrained and enjoined by Order of this Court, immediate and irreparable harm will result from Defendants' ongoing violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030); the CAN-SPAM Act (15 U.S.C. § 7704); the Electronic Communications Privacy Act (18 U.S.C. § 2701); Trademark Infringement, False Designation of Origin, and Trademark Dilution under the Lanham Act (15 U.S.C. §§ 1114 *et seq.*); the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962); and the common law of trespass, conversion, and unjust enrichment. The evidence set forth in Plaintiffs' TRO Application and the accompanying declarations and exhibits, demonstrates that Plaintiffs are likely to prevail on their claim that Defendants have engaged in violations of the foregoing laws by: (1) intentionally accessing and sending malicious software to the protected computers and operating systems of the customers or associated member organizations of Microsoft, FS-ISAC, and NACHA, without authorization, in order to infect those computers and make them part of the Zeus Botnets; (2) sending malicious software to configure, deploy and operate a botnet; (3) sending unsolicited spam e-mail to Microsoft's Hotmail accounts; (4) sending unsolicited spam e-mails that falsely indicate that they are from or approved by

Plaintiffs or their associated member organizations, the purpose of which is to deceive computer users into taking steps that will result in the infection of their computers with botnet code and/or the disclosure of personal and financial account information; (5) stealing personal and financial account information from computer users; (6) using stolen information to steal money from the financial accounts of those users; and (7) associating with one another in a common enterprise engaged in these illegal acts. There is good cause to believe that if such conduct continues, irreparable harm will occur to Plaintiffs and the public, including Plaintiffs' customers and associated member organizations. There is good cause to believe that the Defendants are engaging, and will continue to engage, in such unlawful actions if not immediately restrained from doing so by Order of this Court.

5. There is good cause to believe that immediate and irreparable damage to this Court's ability to grant effective final relief will result from the sale, transfer, or other disposition or concealment by Defendants of the botnet command and control software that is hosted at and otherwise operates through the Internet domains listed in Appendix A, the Internet Protocol (IP) addresses listed in Appendix B, and the file directories listed in Exhibit C, and from the destruction or concealment of other discoverable evidence of Defendants' misconduct available at those locations. Based on the evidence cited in Plaintiffs' TRO Application and accompanying declarations and exhibits, Plaintiffs are likely to be able to prove that: (1) Defendants are engaged in activities that directly violate U.S. law and harm Plaintiffs and the public, including Plaintiffs' customers and member organizations; (2) Defendants have continued their unlawful conduct despite the clear injury to the foregoing interests; (3) Defendants are likely to delete or relocate the botnet command and control software at issue in Plaintiffs' TRO Application and the harmful, malicious, and trademark infringing software disseminated through these IP addresses and domains.

6. There is good cause to believe that Defendants have engaged in illegal activity using the data centers and/or Internet hosting providers identified in Appendix B to host the command and control software and the malicious botnet code and content used to

maintain and operate the botnet at computers, servers, electronic data storage devices or media at the IP addresses identified in Appendix B.

7. There is good cause to believe that to immediately halt the injury caused by Defendants, data and evidence at Defendants' IP addresses identified in Appendix B must be preserved and held in escrow pending further order of the court, Defendants' computing resources related to such IP addresses must then be disconnected from the Internet, Defendants must be prohibited from accessing Defendants' computer resources related to such IP addresses and the data and evidence located on those computer resources must be secured and preserved.

8. There is good cause to believe that Defendants have engaged in illegal activity using the Internet domains identified in Appendix A to this order to host the command and control software and content used to maintain and operate the botnet. There is good cause to believe that to immediately halt the injury caused by Defendants, each of Defendants' current and prospective domains set forth in Appendix A must be immediately redirected to the Microsoft-secured IP address 199.2.137.141, using name servers ns1.microsoftinternetsafety.net and ns2.microsoftinternetsafety.net, or, alternatively, the domain registries, registrars and/or registrants located or with a presence in the United States should take other reasonable steps to work with Plaintiffs to ensure that Defendants cannot use the Appendix A domains to control the botnet. Such reasonable assistance in the implementation of this Order and to prevent frustration of the implementation and purposes of this Order, are authorized pursuant to 28 U.S.C. § 1651(a) (the All Writs Act).

9. This Court respectfully requests, but does not order, that foreign domain registries and registrars take reasonable steps to work with Plaintiffs to ensure that Defendants cannot use the Appendix A domains to control the botnet.

10. There is good cause to permit notice of the instant Order and service of the Complaint by formal and alternative means, given the exigency of the circumstances and the need for prompt relief. The following means of service are authorized by law, satisfy Due



Process, satisfy Fed. R. Civ. Pro. 4(f)(3), and are reasonably calculated to notify Defendants of the instant order, the Preliminary Injunction hearing and of this action: (1) personal delivery upon Defendants who provided to the data centers and Internet hosting providers contact information in the U.S.; (2) personal delivery through the Hague Convention on Service Abroad or other treaties upon Defendants who provided contact information outside the United States; (3) transmission by e-mail, electronic messaging addresses, facsimile, and mail to the known email and messaging addresses of Defendants and to their contact information provided by Defendants to the domain registrars, registries, data centers, Internet hosting providers, and website providers who host the software code associated with the IP addresses in Appendix B, or through which domains in Appendix A are registered; and (4) publishing notice to the Defendants on a publicly available Internet website and in newspapers in jurisdictions where Defendants are believed to reside.

11. There is good cause to believe that the harm to Plaintiffs of denying the relief requested in their request for a Preliminary Injunction outweighs any harm to any legitimate interests of Defendants and that there is no undue burden to any third party.

#### **PRELIMINARY INJUNCTION**

**IT IS THEREFORE ORDERED** as follows:

A. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from: Intentionally accessing and sending malicious software to Plaintiffs and the protected computers and operating systems of Plaintiffs' customers' and associated member organizations, without authorization, in order to infect those computers and make them part of the botnet; sending malicious software to configure, deploy and operate a botnet; sending unsolicited spam e-mail to Microsoft's Hotmail accounts; sending unsolicited spam e-mail that falsely indicate that they are from or approved by Plaintiffs or Plaintiffs' associated member organizations; creating false websites that falsely indicate that they are associated with or approved by Plaintiffs or Plaintiffs' member organizations; or stealing information, money or property

from Plaintiffs, Plaintiffs' customers or Plaintiffs' member organizations, or undertaking any similar activity that inflicts harm on Plaintiffs, or the public, including Plaintiffs' customers or associated member organizations.

B. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from configuring, deploying, operating or otherwise participating in or facilitating the botnets described in the TRO Application, including but not limited to the command and control software hosted at and operating through the domains and IP addresses set forth herein and through any other component or element of the botnets in any location.

C. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from using the trademarks "Microsoft," "Windows," "Outlook," "NACHA," the NACHA logo, trademarks of financial institution members of FS-ISAC and/or other trademarks; trade names; service marks; or Internet Domain addresses or names; or acting in any other manner which suggests in any way that Defendants' products or services come from or are somehow sponsored or affiliated with Plaintiffs or Plaintiffs' associated member organizations, and from otherwise unfairly competing with Plaintiffs, misappropriating that which rightfully belongs to Plaintiffs or Plaintiffs' customers or Plaintiffs' associated member organizations, or passing off their goods or services as Plaintiffs or Plaintiffs' associated member organizations.

D. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from infringing Plaintiffs' registered trademarks, Registration Nos. 2872708, 85467641, 2463510, 3419145 and others.

E. Defendants, their representatives and persons who are in active concert or participation with them are temporarily restrained and enjoined from using in connection with Defendants' activities any false or deceptive designation, representation or description of Defendants' or of their representatives' activities, whether by symbols, words, designs or statements, which would damage or injure Plaintiffs or give Defendants an unfair

competitive advantage or result in deception of consumers.

F. Defendants' materials bearing infringing marks, the means of making the counterfeit marks, and records documenting the manufacture, sale, or receipt of things involved in such violation, in the possession of data centers operated by Continuum Data Centers LLC and Burstnet Technologies, Inc., which have been seized pursuant to 15 U.S.C. §1116(d), shall be held in secure escrow by Stroz Friedberg, 1925 Century Park East, Suite 1350, Los Angeles, CA 90067, which will act as substitute custodian of any and all data and properties seized and evidence preserved pursuant to this Order. Such materials shall be stored securely and not accessed by any party until further order of this Court.

G. The registries of the domains identified in Exhibit A to this Order (the "Registries") shall implement the provisions of this order in the following fashion:

1. For currently registered domains, the domain name registrant information and point of contact shall not be changed and associated WHOIS information shall not be changed;
2. Domain names shall not be deleted or otherwise made available for registration by any party, but rather should remain active and redirected to IP address 199.2.137.141, using name servers ns1.microsoftinternetsafety.net and ns2.microsoftinternetsafety.net.
3. Domains shall not be transferred to any other person or registrar, pending further order of the court;
4. The Registries shall assume authority for name resolution of domain names to IP address 199.2.137.141, using the name servers ns1.microsoftinternetsafety.net and ns2.microsoftinternetsafety.net;
5. Name resolution services shall not be suspended;
6. The Registries and Plaintiffs shall otherwise work together in good faith to take any other reasonable steps necessary to prevent Defendants from using the Appendix A domains.



H. Defendants are directed to permanently disable access to the file paths identified in Appendix C; permanently delete or otherwise disable the content at those file paths; and take all necessary steps to ensure that such file paths are not re-enabled nor the content recreated. Pursuant to the All Writs Act, U.S. based free website hosting providers of the domains set forth in Appendix C are directed to permanently delete or otherwise disable the content at the file paths in Appendix C.

**IT IS FURTHER ORDERED**, that copies of this Order, notice of the Preliminary Injunction hearing and service of the Complaint may be served by any means authorized by law, including (1) by personal delivery upon defendants who provided contact information in the U.S.; (2) personal delivery through the Hague Convention on Service Abroad upon defendants who provided contact information outside the U.S.; (3) by transmission by e-mail, electronic messaging addresses, facsimile and mail to the known contact information of Defendants and to such contact information provided by defendants to the data centers, Internet hosting providers and domain registrars who hosted the software code associated with the IP addresses set forth at Appendix B or through which domains in Appendix A are registered; and (4) by publishing notice to Defendants on a publicly available Internet website or in newspapers in the jurisdictions where Defendants are believed to reside.

**IT IS FURTHER ORDERED** that Plaintiffs shall post bond in the amount of \$300,000 as cash to be paid into the Court registry.

**IT IS FURTHER ORDERED** that Plaintiffs shall compensate the data centers, Internet hosting providers and/or domain registries and/or website providers identified in Appendices A, B and C at prevailing rates for technical assistance rendered in implementing the Order.

**IT IS FURTHER ORDERED** that this Order shall be implemented with the least degree of interference with the normal operation of the data centers and Internet hosting providers and/or domain registries and/or website providers identified in Appendices A, B and C consistent with thorough and prompt implementation of this Order.

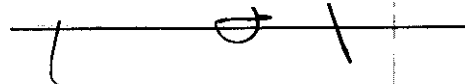
**IT IS FURTHER ORDERED**, specifically with regard to the preserved Internet traffic to and from the servers corresponding to the IP addresses listed in Exhibit B, that this evidence shall be preserved, held in escrow and kept under seal by Stroz Friedberg, and not accessed by any party, pending further order of this Court.

**IT IS FURTHER ORDERED**, specifically with regard to the Internet traffic that is redirected from the domains listed in Exhibit A to the Microsoft-secured IP address 199.2.137.141, using name servers ns1.microsoftinternetsafety.net and ns2.microsoftinternetsafety.net, that Microsoft shall not record more than the IP addresses of incoming connections.

**IT IS SO ORDERED**

Entered this <sup>th</sup>29 day of March, 2012.

/s/(SJ)

A handwritten signature, likely of Stroz Friedberg, is written over a horizontal line. The signature is stylized and appears to be a cursive or semi-cursive script.